Abstract

The inventive method is based on a publicly known mathematical number group (G) and a higher order element of the group g ∈ G. In the first work step, a message corresponding to Ni: = $g^{zi}$ mod p) is sent by each subscriber (Ti) to all other subscribers (Tj), (zi) being a random number chosen from the set (1, ..., p-2) by a random number generator. In the second work step, each subscriber (Ti) selects a transmission key kij: = $(g^{zj})^{zi}$ for each other subscriber (Tj) from the received message ($g^{zj}$), with i ≠ j, for transmitting their random number (zi) to the subscribers (Tj). In the third work step, the common key k is calculated as k: = f(z1, z2, ..., zn) for each subscriber Ti. The inventive method can be advantageously used for generating a cryptographic key for a group of at least three subscribers.